RAPPORT

État des lieux 2023 des technologies OT et de leur cybersécurité

FORTINET

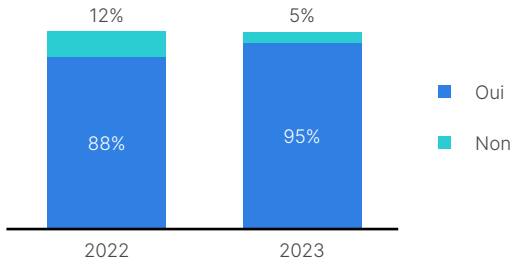
Table des matières

L'essentiel

Collaborateurs

Dans presque toutes les entreprises interrogées, les DSSI sont désormais (ou seront bientôt) responsables de la cybersécurité des systèmes industriels OT (Operational Technology). Notons également que les professionnels de la cybersécurité OT sont davantage issus de la direction de la sécurité informatique que des équipes opérationnelles.

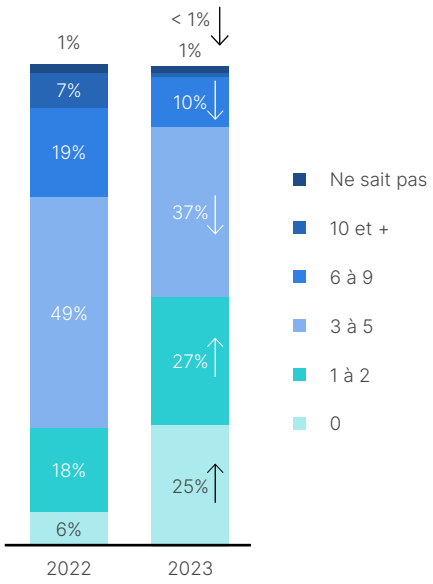
La cybersécurité relèvera de la responsabilité du DSSI dans les 12 mois à venir



Incidents de cybersécurité

Si le nombre d'entreprises n'ayant subi aucune intrusion de cybersécurité est en net progrès depuis l'an dernier (de 6% en 2022 à **25% en 2023**), les axes d'amélioration restent nombreux. 3/4 des acteurs industriels signalent au moins une intrusion au cours de l'année écoulée, et près d'un tiers des personnes interrogées déclarent avoir été victimes d'une attaque par ransomware (**32%**, comme en 2022). Les intrusions dues à des logiciels malveillants et au phishing ont progressé de **12%** et de **9%** respectivement.

Nombre d'intrusions au cours de l'année écoulée



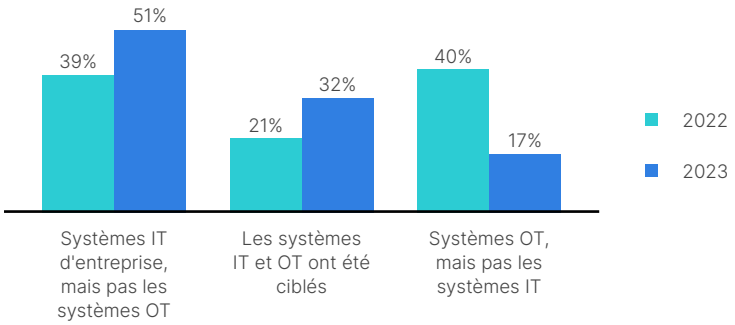
Intrusions par degré de maturité en cybersécurité

	Niveau 0–2	Niveau 3	Niveau 4
Ne sait pas	1%	0%	0%
10 et +	1%	2%	0%
6 à 9	11%	11%	6%
3 à 5	38%	35%	40%
1 à 2	36%[B]	21%	25%
0	14%	31%[A]	29%[A]

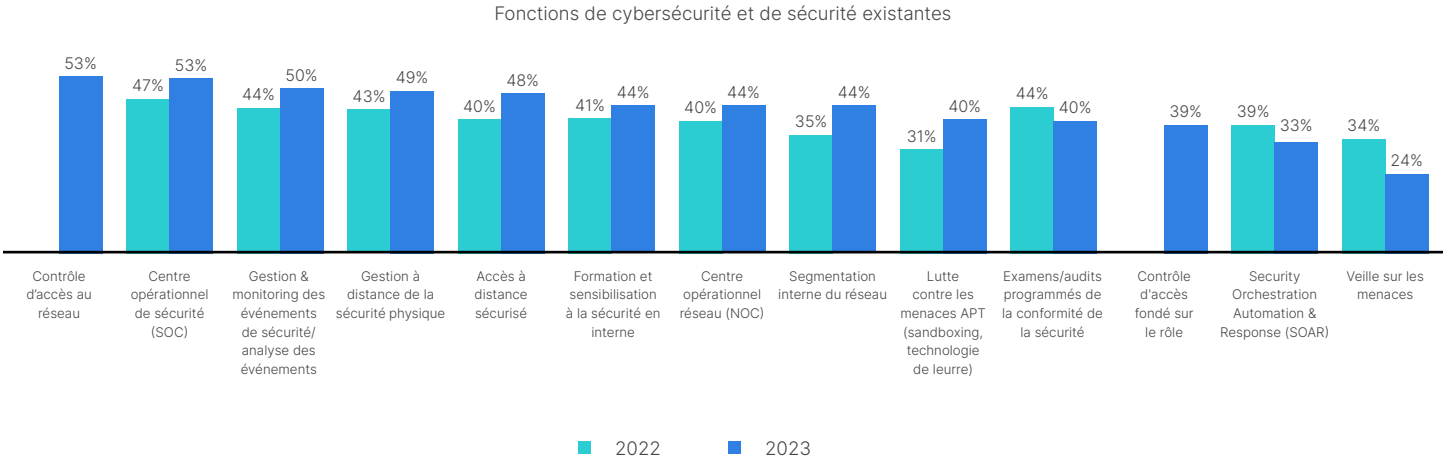
L'impact des intrusions

En cas de cyberattaque en début d'année, près d'un tiers **(32%)** des personnes interrogées indiquent que leurs systèmes IT et OT ont été tous les deux ciblés, contre seulement 21% l'année dernière. Pour lutter contre les intrusions, les professionnels de l'OT déploient des solutions de cybersécurité supplémentaires au sein de leurs réseaux industriels.

Environnements impactés

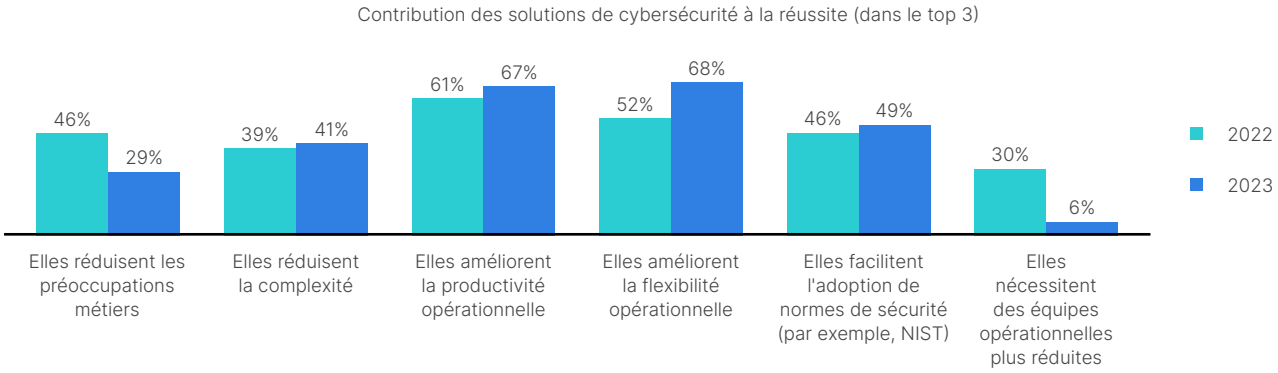


Les menaces APT, la segmentation du réseau interne et l'accès à distance sécurisé affichent les plus solides progressions, tandis que la veille sur les menaces, en tant que solution, est en repli.



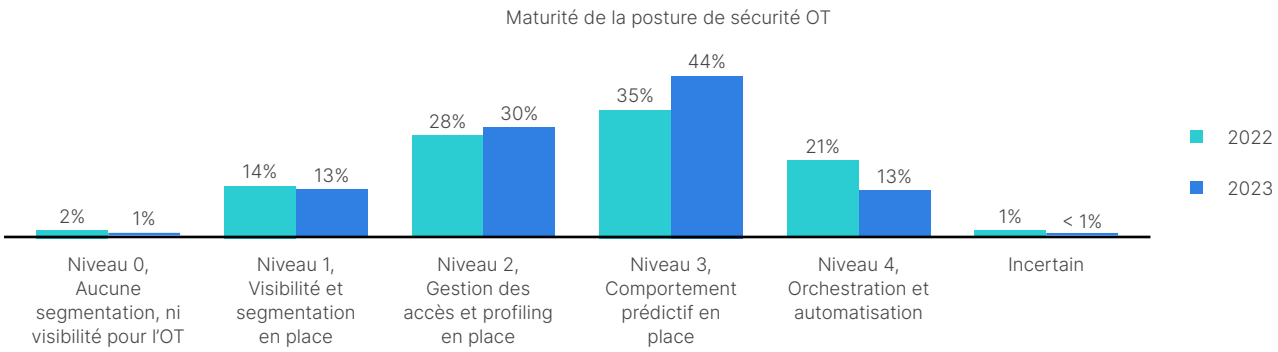
La cybersécurité, facteur de succès

Si les résultats de l'enquête révèlent que les solutions de cybersécurité contribuent à la réussite de la plupart **(76%)** des professionnels de l'OT, notamment en améliorant leur productivité **(67%)** et leur flexibilité **(68%)**, les données attestent également que la prolifération des solutions rend plus complexe une protection cohérente des environnements IT/OT convergents.

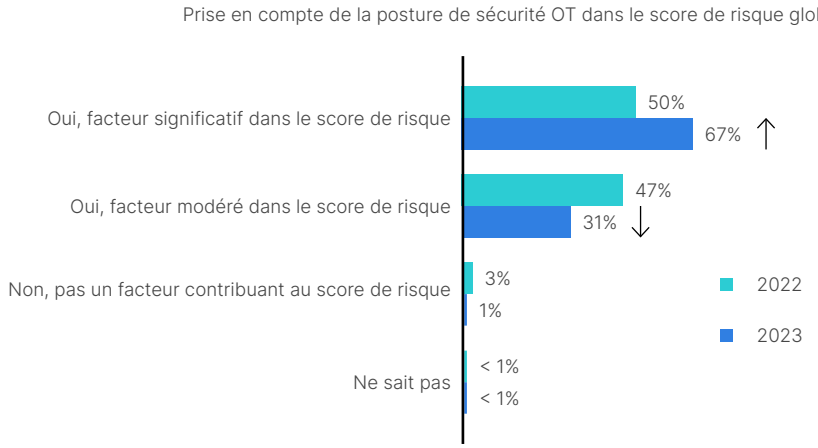


Posture de cybersécurité

La part des entreprises qui qualifient la posture de cybersécurité OT de leur entreprise de niveau 4 ("très mature") recule cette année par rapport à 2022 (**13% contre 21%**). **44%** des entreprises s'estiment désormais au niveau 3, contre 35% l'année dernière, ce qui peut refléter une évaluation plus pertinente de leur posture et une vision plus réaliste de cette posture.



Presque toutes les entreprises (98%) intègrent désormais la posture de cybersécurité OT dans l'évaluation du score de risque présenté aux dirigeants d'entreprise et au conseil d'administration.

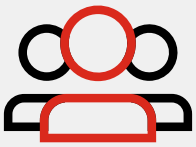


Synthèse

L'état des lieux 2023 des technologies OT et de leur cybersécurité est notre cinquième étude annuelle basée sur les résultats d'une enquête mondiale menée auprès de 570 professionnels des technologies OT par un spécialiste reconnu des études de marché.

La protection des systèmes OT est aujourd'hui un sujet plus critique que jamais, de plus en plus d'entreprises connectant leurs environnements OT à Internet. Bien que la convergence IT/OT présente de nombreux avantages, elle s'expose à des cybermenaces sophistiquées et destructrices. Les conséquences de ces attaques portent de plus en plus sur les environnements OT. Pour ces raisons, les données de l'enquête de cette année indiquent que la cybersécurité OT est aujourd'hui un élément plus crucial dans la gestion des risques d'une entreprise.

L'analyse des données de 2023 révèle quatre grandes tendances mondiales :



Le rapport de 2023 révèle que 95% des organisations ont confié à leur DSSI la responsabilité de leur cybersécurité OT.

- Le nombre d'intrusions est, globalement, en repli en raison de la baisse du nombre de violations par des initiés, bien que les ransomwares et le phishing restent des menaces importantes. Cette baisse résulterait davantage d'une approche plus ciblée adoptée par les cybercriminels, plutôt que d'un repli du niveau du risque cyber.
- Presque toutes les entreprises ont confié la responsabilité de leur cybersécurité OT à un DSSI plutôt qu'à un cadre ou à une équipe opérationnelle.
- Les entreprises et les professionnels de l'OT disposent d'un large parc de solutions de cybersécurité pour lutter contre les intrusions. Il semblerait que les produits de sécurité autonomes et cloisonnés, ainsi que leur prolifération, rendent plus difficile une mise en œuvre cohérente des politiques dans l'univers convergent de l'IT et de l'OT.
- Le nombre de répondants qui considèrent que la maturité de leur entreprise en matière de cybersécurité est de niveau 4 passe de 21%, il y a un an, à 13% aujourd'hui, tandis que la part de ceux qui estiment que leur cybersécurité est de niveau 3 progresse de 35% à 44%. Cette évolution semble indiquer que les professionnels OT assurent une auto-évaluation plus réaliste des capacités de leur entreprise en matière de cybersécurité OT.

Après cinq années d'enquête auprès des professionnels OT, la nouvelle la plus encourageante est que la cybersécurité semble enfin sortir de l'ombre. La cybersécurité OT fait désormais l'objet d'une attention marquée de la part des dirigeants d'entreprise. Cependant, la plupart des entreprises ont encore beaucoup de travail à faire, d'autant qu'il n'est jamais conseillé de se reposer sur ses lauriers en matière de cybersécurité.

Pour étayer la posture de sécurité OT de votre entreprise, l'état des lieux de cette année sur la cybersécurité OT présente une liste des meilleures pratiques communes que les organisations de premier plan mettent en œuvre pour assurer la sécurité de leurs systèmes OT.

Introduction

Aujourd'hui, personne ne doute de l'importance de la protection des systèmes OT. Les technologies OT contrôlent les infrastructures critiques dont nous dépendons tous - de la gestion des réseaux électriques à l'exploitation des systèmes d'eau et d'égouts, du fonctionnement des réseaux de transport à la production de biens industriels et à la mise en place de chaînes d'approvisionnement mondiales. N'oublions pas également que l'OT fait partie des projets d'accélération digitale de nombreux acteurs industriels.

Les conditions actuelles du marché ont encouragé l'adoption des méthodologies et technologies de l'industrie 4.0 et ont abouti à une « ère de connectivité, de traitement analytique sophistiqué, d'automatisation et de technologies de production avancée »[1], essentielle à la préservation des avantages concurrentiels des industriels.

Menaces de sécurité sur l'OT

La convergence des réseaux IT et OT attire l'attention des cybercriminels et de certains États-nations belliqueux. Les récents rapports sur les menaces mondiales de FortiGuard Labs soulignent une détection accrue de malwares et d'activités malveillantes au sein des systèmes OT.[2]

Plusieurs attaques de cybersécurité très médiatisées ont été le signal d'alarme pour les responsables de la protection des systèmes OT. Les exactions permanentes de la Russie contre les infrastructures critiques de l'Ukraine[3], qui a dégénéré en une guerre physique il y a déjà plus d'un an, en sont un excellent exemple[4]. Les systèmes OT du monde entier continuent d'être la cible des cybercriminels, en particulier dans le secteur de la production industrielle qui continue de subir de nombreuses attaques ciblées par ransomware contre ces systèmes OT[5]

La part des entreprises ayant subi une intrusion par ransomware dans l'enquête de cette année (32%) reste la même par rapport à l'année précédente. La ligne de défense contre ces types d'attaque doit se renforcer. Compte tenu de l'évolution et de la sophistication croissante des opérations de ransomware, il n'est guère surprenant que 84% du panel de l'enquête Fortinet 2023 Global Ransomware Report de cette année restent " très " ou " extrêmement " préoccupés par cette menace.[6]

Si les intrusions intentionnelles et non intentionnelles d'initiés ont considérablement reculé cette année selon les personnes interrogées, les intrusions dues aux logiciels malveillants et au phishing ont progressé, respectivement de 12% et 9%. Les résultats de l'enquête sont confirmés par le dernier rapport mondial sur les menaces de FortiGuard Labs, qui indique que "les logiciels malveillants font souvent la une de l'actualité, ce qui incite les entreprises à être sur le qui-vive"[7].

Un environnement OT décloisonné

Avec des infrastructures IT et OT plus étroitement intégrées, le cloisonnement qui, auparavant, protégeait les systèmes OT des cyberattaques, n'est plus d'actualité. Par conséquent, la surface d'attaque des entreprises industrielles s'est considérablement élargie. La présence plus importante des dispositifs de l'Internet industriel des objets (IIoT), la sensibilité accrue de l'OT aux menaces IT et la valeur plus importante que représentent les environnements de production aux yeux des cybercriminels sont autant de raisons qui incitent les industriels à payer une rançon en cas d'infection par un rançongiciel. Dans ce contexte, la protection de l'OT est devenue d'autant plus essentielle.

La cybersécurité OT sous les feux de la rampe

L'état des lieux dressé l'an dernier sur les technologies OT et leur cybersécurité [8] validait la pertinence d'investir davantage dans la cybersécurité OT. Toutefois, comme le révèle le rapport de cette année, de nombreuses entreprises ont encore un long chemin à parcourir pour protéger de manière adéquate leurs systèmes OT.

Plongeons dans les données de l'enquête de cette année et voyons ce que nous pouvons apprendre sur l'état actuel de la cybersécurité OT. Nous espérons que notre étude de l'année prochaine indiquera des progrès significatifs réalisés en matière de protection des systèmes OT.

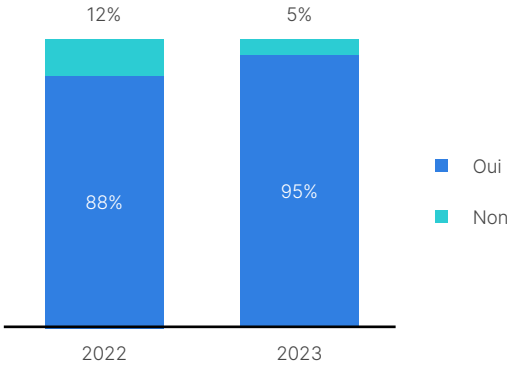
Perspectives clés

Perspective n° 1 : les responsabilités en matière de cybersécurité OT migrent des équipes OT vers des experts en cybersécurité

Les collaborateurs qui évoluent dans le domaine des technologies OT sont présents dans presque tous les grands secteurs d'activité : production industrielle, transport, logistique, soins de santé, industrie pharmaceutique, pétrole, gaz, énergie, services publics, industrie chimique, eau, eaux usées, etc. Traditionnellement, ces professionnels de l'OT ont été impliqués dans les décisions d'achat pour leurs environnements OT.

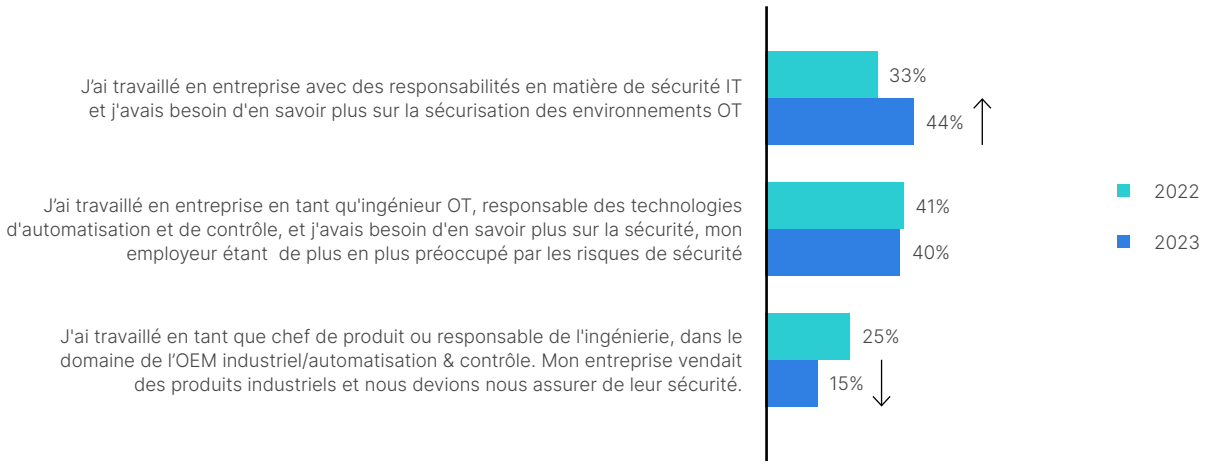
Cependant, il semble que la vulnérabilité des réseaux OT aux cyberattaques ait conduit à progressivement faire de la cybersécurité OT une responsabilité du DSSI. Les données montrent également que les professionnels de la sécurité OT proviennent des rangs de l'équipe IT plutôt que de profils de gestion de produits et de la production. En conséquence, et comme l'indiquent les données de l'enquête, les cadres dirigeants et les décideurs traditionnels en matière de sécurité, en particulier les DSSI, s'impliquent et s'investissent davantage dans la prise de décision en matière de cybersécurité.

Q : Votre entreprise prévoit-elle de confier sa cybersécurité OT au DSSI au cours des 12 prochains mois ?



La cybersécurité relèvera de la responsabilité du DSSI dans les 12 mois à venir

Q : Quel est le parcours professionnel qui vous a mené à la sécurité OT ?

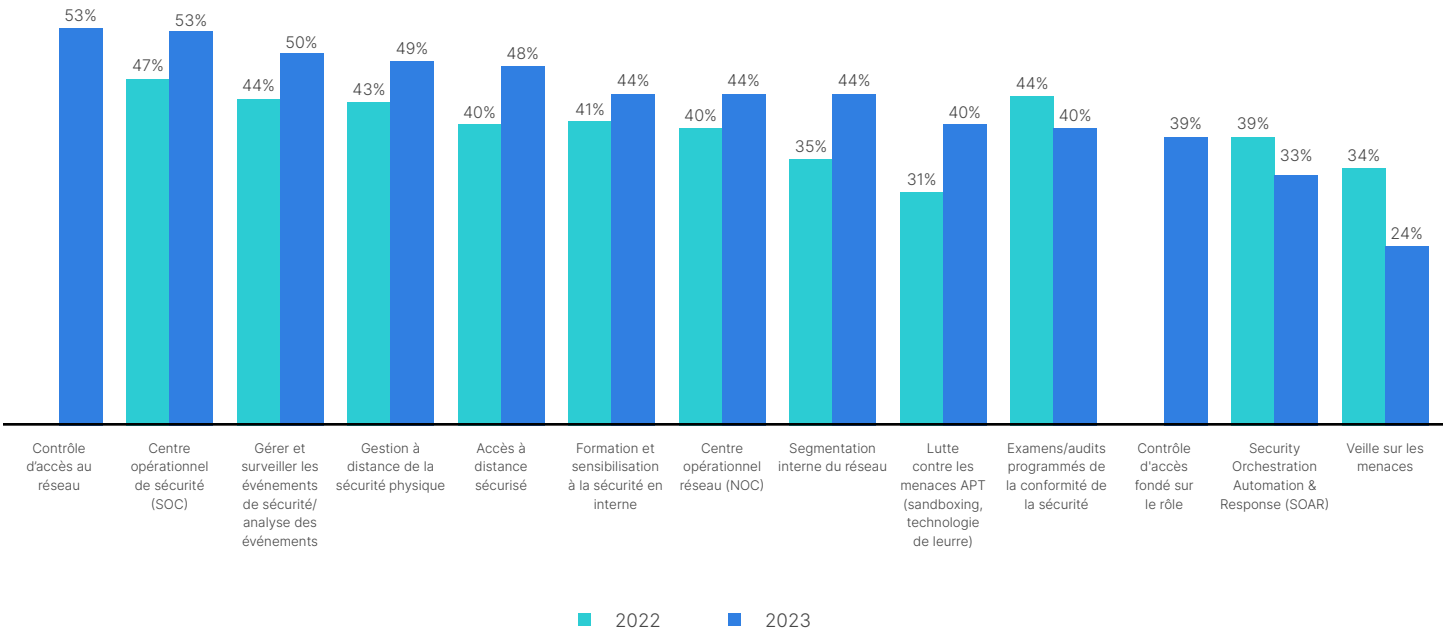


Parcours professionnel ayant mené à la sécurité OT

Perspective 2 : les professionnels OT font appel à un panel de solutions

Cette année, les professionnels OT interrogés recherchent des solutions de cybersécurité capables, avant toute chose, de détecter les vulnérabilités connues. Les équipes OT sont confrontées à un défi unique, à savoir les temps d'indisponibilité, souvent beaucoup plus critiques que dans les environnements IT. Par conséquent, le succès d'un réseau OT se mesure moins par la confidentialité et de l'intégrité des données sur le long terme que par la disponibilité des systèmes critiques. D'où l'intérêt de mettre l'accent sur les délais de réponse aux attaques, comme l'illustre le déploiement de solutions de cybersécurité et de réseaux OT.

Toutefois, comme pour les réseaux IT, déployer de nouvelles solutions ne suffit pas à prévenir toutes les attaques sur les réseaux OT. Une partie du défi résulte de la prolifération des produits et des fournisseurs au sein de l'arsenal de défense, ce qui rend plus difficile la détection d'une menace et freine toute réponse coordonnée.



Fonctions de cybersécurité et de sécurité existantes

Perspective 3 : les intrusions restent préoccupantes

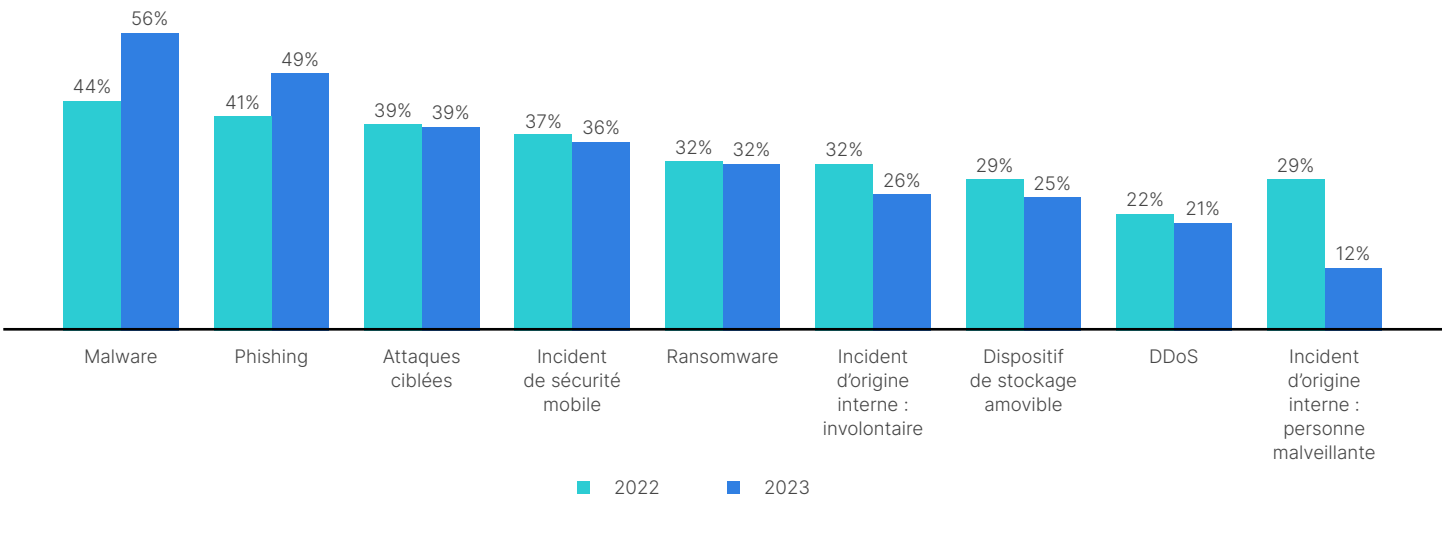
Le nombre d'intrusions est en baisse, mais 75 % des entreprises interrogées déclarent avoir subi au moins une intrusion au cours des 12 derniers mois. Cette baisse globale est attribuée à une diminution du nombre d'incidents d'origine interne, et non à des attaques cybercriminelles moins nombreuses.

Cependant, les incidents liés aux malwares et au phishing comptent parmi les menaces les plus courantes et ont progressé sur un an. Et les ransomwares restent la plus préoccupation la plus critique, avec un nombre d'exactions qui continue à progresser. Les impacts sont multiples, affectant de plus en plus les systèmes IT et OT. La restauration post-incident a cependant tendance à s'effectuer en quelques heures et, de plus en plus souvent, en quelques minutes.

La baisse des intrusions résulte, en partie, d'un changement dans les tactiques employées par les cybercriminels. Cependant, les approches des assaillants restent efficaces si l'on en croit la recrudescence des malwares et du phishing. Néanmoins, compte tenu de la valeur élevée des systèmes OT, nous pouvons prévoir une évolution vers des attaques plus ciblées.

Il est important de noter qu'un excès de confiance dans l'état de préparation nuit aux organisations, tout autant que l'utilisation de technologies inadaptées. Selon notre dernier rapport sur les ransomwares,[9] si la lutte contre les ransomwares reste une priorité pour la plupart des entreprises, de nombreuses solutions qu'elles considèrent comme essentielles à leur stratégie de cybersécurité offrent une protection médiocre contre les attaques par ransomware.

Q : Quels types d'intrusion ont été constatés (cochez toutes les cases pertinentes) ?



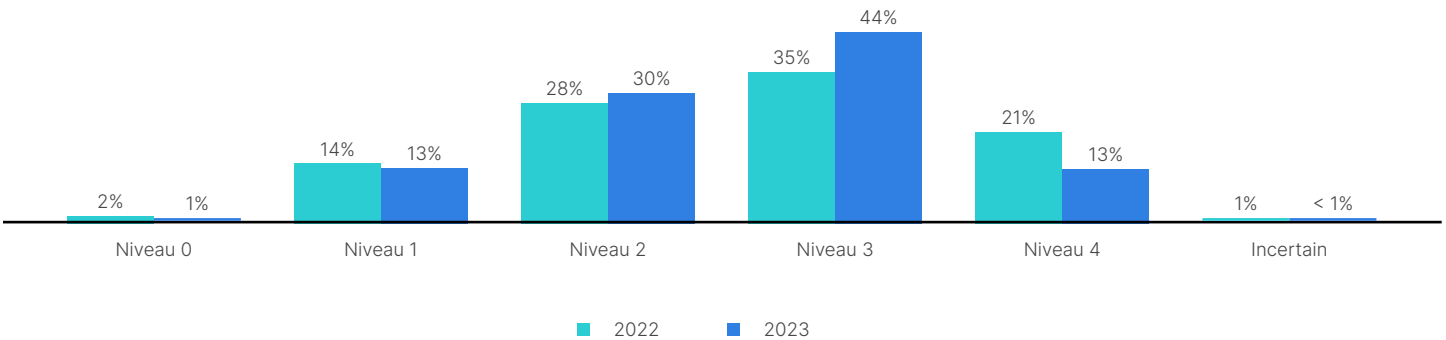
Intrusions constatées

Perspective 4 : le niveau moyen de la maturité en cybersécurité s'améliore

Une auto-évaluation précise des capacités de cybersécurité et de la maturité de la posture est une première étape essentielle pour améliorer les cyberdéfenses et sécuriser efficacement les environnements OT. Globalement, cette année, les entreprises sont moins nombreuses à qualifier leur posture de sécurité OT comme très mature, avec un chiffre qui passe de 21% en 2022 à 13% cette année. Dans le même temps, 44% des entreprises évaluent désormais la maturité de leur posture de cybersécurité OT à un niveau 3, contre 35% il y a un an. Ces données indiquent que les répondants de cette année ont peut-être évalué de manière plus réaliste leurs capacités de cybersécurité OT.

L'échelle de maturité	
Niveau 0	Aucune segmentation, ni visibilité pour l'OT
Niveau 1	Visibilité et segmentation en place
Niveau 2	Accès et profiling en place
Niveau 3	Comportement prédictif en place
Niveau 4	Orchestration et automatisation

Q : Comment caractériseriez-vous la maturité de votre posture de sécurité OT ?

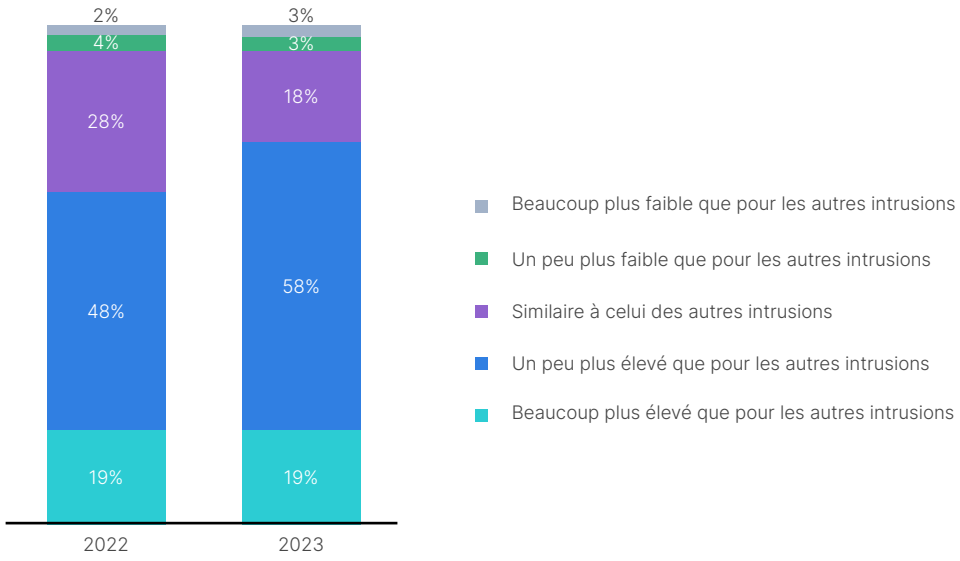


Maturité de la posture de sécurité OT

Au cœur de l'enquête 2023

Q : Par rapport à d'autres incidents, dans quelle mesure êtes-vous préoccupé par l'impact des ransomwares sur votre environnement OT ?

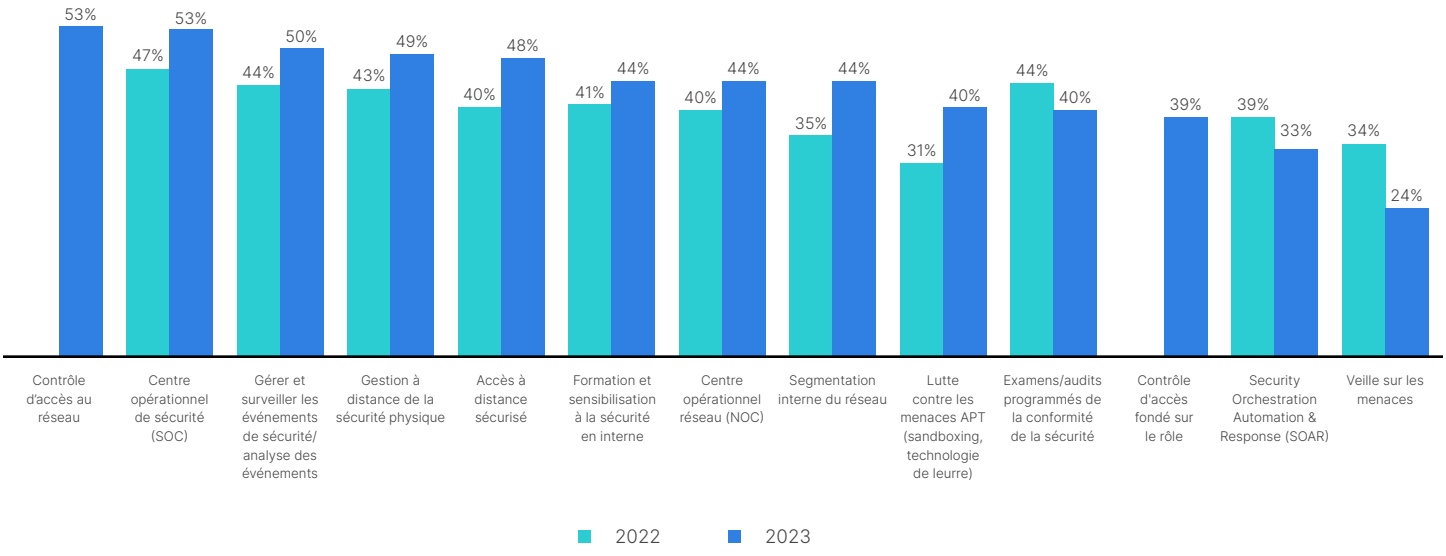
Les incidents liés aux ransomwares survenant sur le réseau IT d'entreprise peuvent avoir un impact direct ou indirect sur l'outil de production. Les entreprises sont de plus en plus préoccupées par ce type d'intrusion (même si le phishing et les logiciels malveillants sont plus courants). Les ransomwares restent donc une préoccupation majeure en raison de leurs conséquences sur la production et sur le plan financier.



Préoccupations quant à l'impact des rançongiciels

Q : Quels sont vos dispositifs de cybersécurité et de sécurité actifs aujourd'hui ?

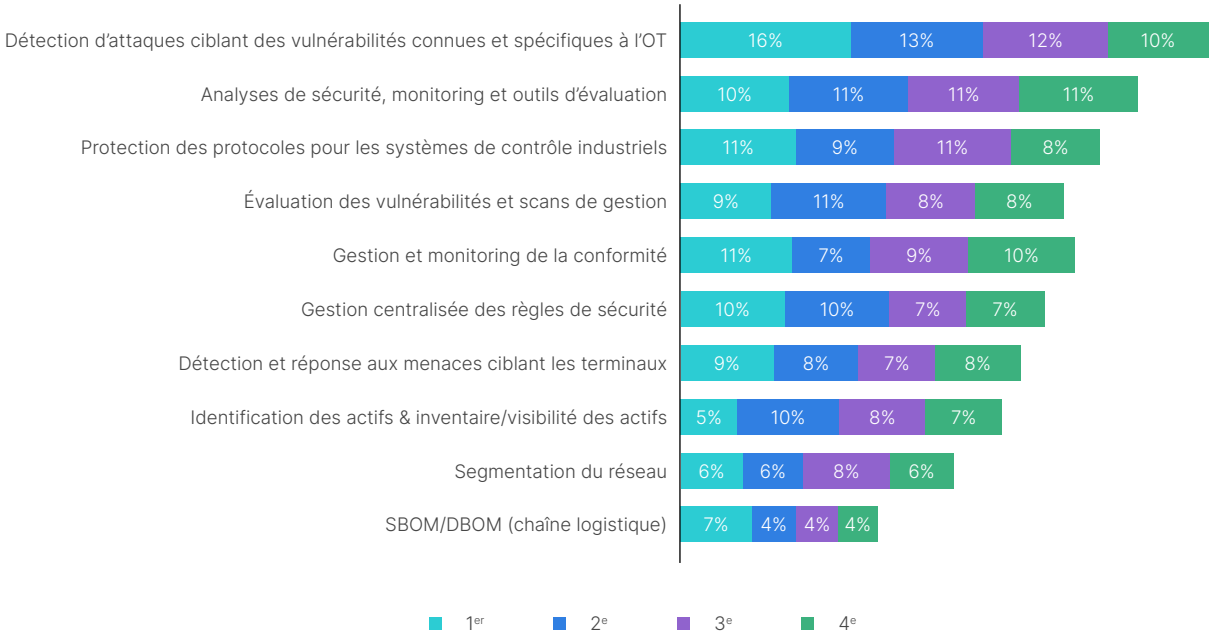
Pour lutter contre les intrusions, les professionnels de l'OT renforcent les nombreux dispositifs de cybersécurité et de défense déployés. Nous pensons que les audits de sécurité ont été moins nombreux en raison de la prolifération de ces dispositifs supplémentaires et de solutions plus avancées portant notamment sur le SOAR et la veille sur les menaces. Une fois que ces nouveaux dispositifs seront opérationnels, les audits devraient être plus nombreux, jusqu'à probablement atteindre les niveaux précédents.



Fonctions de cybersécurité et de sécurité existantes

Q : Quelles sont les caractéristiques les plus importantes pour les solutions de cybersécurité d'OT (classez jusqu'à 4 d'entre elles) ?

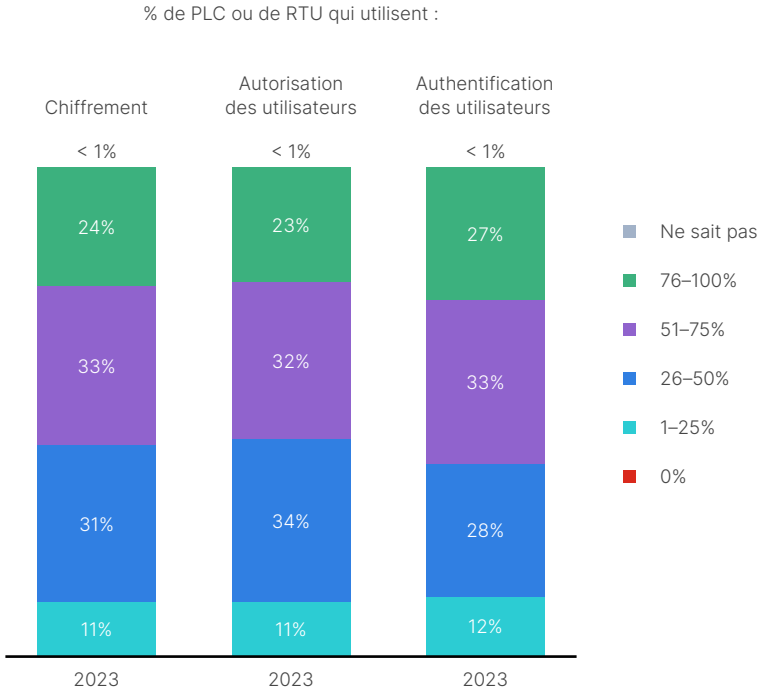
La détection des attaques qui exploitent des vulnérabilités connues est désormais la fonction la plus essentielle de cybersécurité, d'autant que son importance a progressé au cours de l'année écoulée. Une autre indication de la maturité croissante de la sécurité OT est la moindre priorité accordée à l'identification et la segmentation des ressources. Ce que nous avons constaté est conforme aux recommandations du guide CIS Critical Security Controls ICS[10] : la plupart des entreprises ont pris ces mesures de base et passent à des solutions fondamentales et organisationnelles plus évoluées.



Fonctionnalités les plus importantes des solutions de cybersécurité (classement)

Q : Quelle est la part de vos PLC et RTU qui utilisent chacune des capacités de sécurité suivantes ?

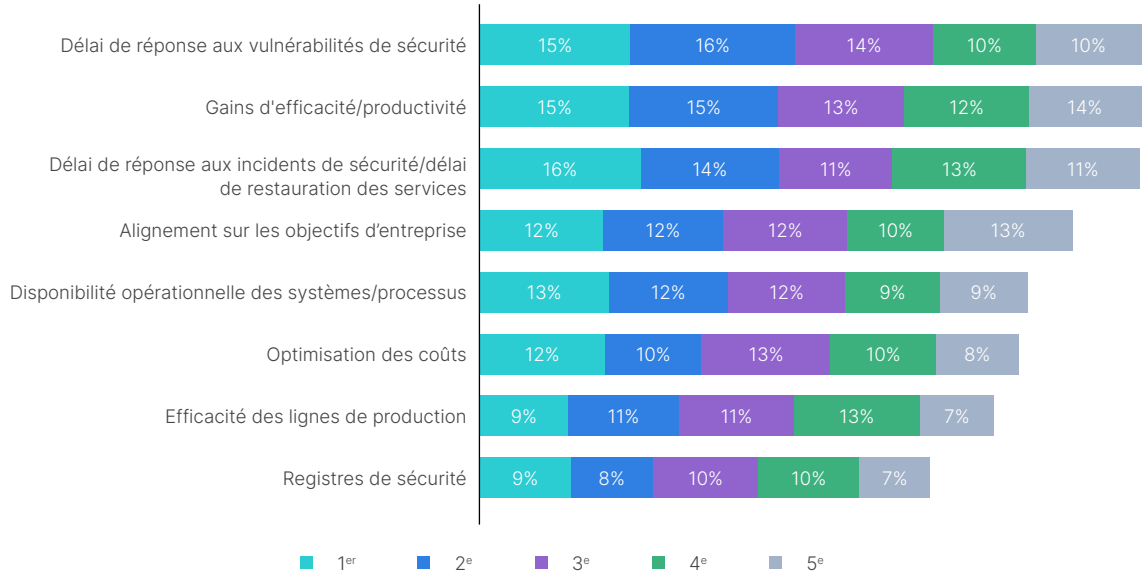
Le chiffrement, l'autorisation des utilisateurs et l'authentification des utilisateurs tendent à être utilisés dans plus de 50 % des PLC (automates programmables industriels) ou RTU (unité terminale distante).



Impact global

Q : Comment mesurez-vous votre réussite ? (jusqu'à cinq réponses)

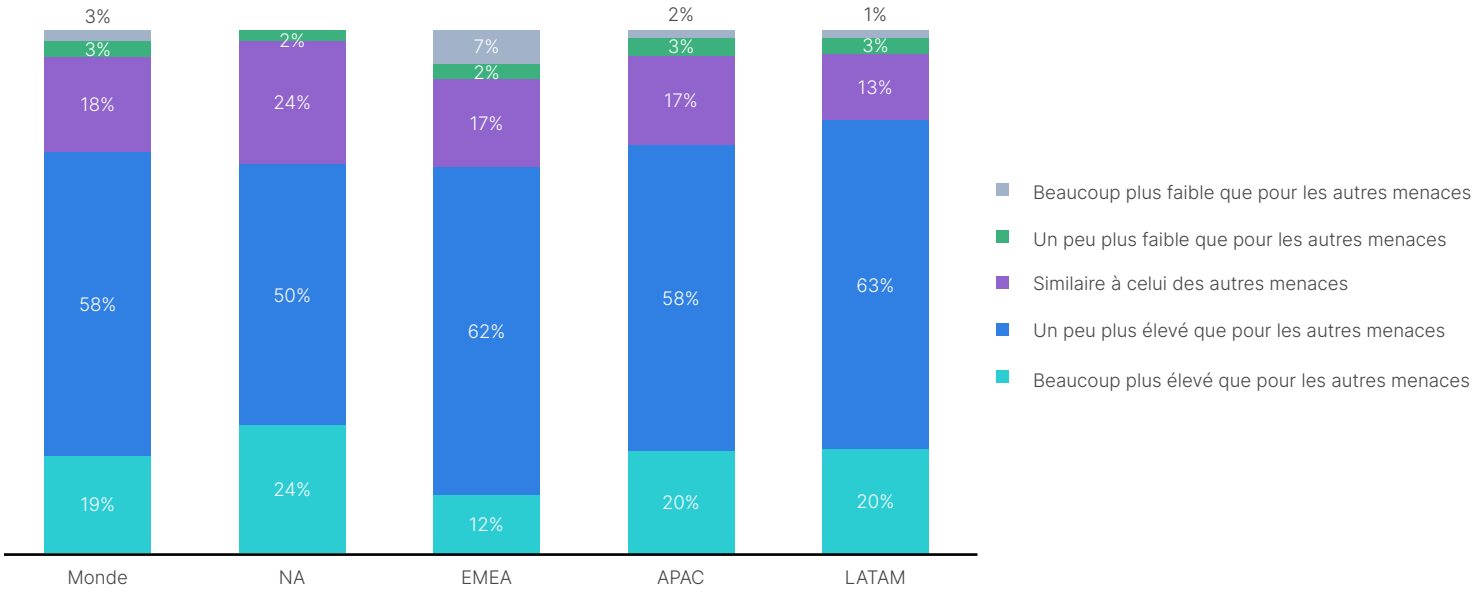
Il est intéressant de noter qu'il n'existe pas de définition unique de la réussite en matière d'OT, ce qui témoigne d'une certaine immaturité de la sécurité OT. Cependant, comme on peut s'y attendre pour les environnements OT, le temps de réponse et les gains de productivité sont les critères les plus essentiels.



Indicateurs de réussite (classement)

Q : Par rapport à d'autres incidents, dans quelle mesure êtes-vous préoccupé par l'impact des ransomwares sur votre environnement OT ?

Bien que les attaques par ransomware ne constituent pas les incidents les plus courants, elles sont la principale préoccupation pour la plupart des entreprises dans le monde (plus que toute autre menace), probablement en raison de leur notoriété et du coût élevé de la restauration des systèmes affectés.



Préoccupations quant à l'impact des rançongiciels

Bonnes pratiques

75 % des entreprises interrogées signalent au moins une intrusion au cours des 12 derniers mois. Ce chiffre, bien qu'élevé, révèle une amélioration par rapport à 2022, où plus de 90% du panel avaient signalé au moins une intrusion. Cette année, seuls 11% des répondants ont signalé six intrusions ou plus, contre 27% l'année dernière.

Alors que les solutions de cybersécurité continuent de contribuer au succès de la plupart (76%) des professionnels de l'OT, notamment en améliorant la productivité (67%) et la flexibilité (68%), les données du rapport indiquent également que la prolifération des solutions rend difficile l'intégration, l'utilisation et l'application cohérentes des politiques au sein de leur environnement IT/OT de plus en plus convergent. La problématique est accentuée par le vieillissement des systèmes, la majorité (74%) des entreprises déclarant que l'âge moyen des systèmes ICS déployés au sein de leur organisation est compris entre six et dix ans. Il ne fait aucun doute que des progrès ont été réalisés dans la cybersécurité OT mondiale, mais les entreprises doivent continuer à aller de l'avant.

Voici quelques-unes des bonnes pratiques qui sont probablement à l'origine de l'amélioration des résultats de l'enquête de cette année.

Élaborer une stratégie de plateforme consolidée pour la cybersécurité OT

La consolidation réduit la complexité et accélère les résultats. La première étape consiste à bâtir une plateforme au fil du temps en faisant appel à des fournisseurs de technologies qui proposent leurs produits dans une optique d'intégration et d'automatisation. Un fournisseur idéal permettra aux entreprises d'incorporer et d'appliquer des politiques de manière cohérente dans un univers IT/OT de plus en plus convergent. Vous pouvez également vous rapprocher de fournisseurs disposant d'un large portefeuille de produits, et qui peuvent fournir des solutions de base pour répertorier et segmenter les ressources,ou des solutions plus sophistiquées, à l'instar d'un SOC dédié à l'OT, voire un SOC commun IT/OT.

Contrôle des accès au réseau (NAC)

Les défis de la sécurisation des systèmes de contrôle industriel (ICS), des systèmes SCADA (supervision et de l'acquisition de données), de l'Internet des objets (IoT), des terminaux BYOD (bring your own device) et des autres terminaux exigent de faire appel à un contrôle d'accès réseau pertinent. Une solution NAC efficace permet également de garder la main sur le réseau d'une entreprise, en gérant les nouveaux appareils qui veulent se connecter ou communiquer avec d'autres parties de l'infrastructure de l'organisation.

Adopter une approche Zero Trust

Mettre en œuvre les étapes de base d'inventaire et de segmentation des ressources. L'accès Zero Trust permet une vérification continue de tous les utilisateurs, applications et appareils cherchant à accéder aux ressources critiques, quel que soit l'endroit où ils se trouvent.

Former et sensibiliser à la sécurité

La formation à la cybersécurité reste essentielle car la lutte contre les cybercriminels nécessite l'implication de tous les collaborateurs, qui devront disposer des connaissances et de la formation nécessaires pour travailler ensemble à leur protection et à celle des données de leur entreprise. Les entreprises sont invitées à proposer des formations non techniques destinées à tous ceux qui utilisent un ordinateur ou un appareil mobile, télétravailleurs et leur famille inclus.

Conseils d'expert

1. Continuer à mettre en œuvre les étapes de base d'inventaire et de la segmentation des actifs, puis utiliser des solutions plus avancées de microsegmentation et de correction virtuelle pour protéger les appareils contre les vulnérabilités connues, afin de disposer de suffisamment de temps pour corriger les appareils correctement.
2. Collaborer avec les équipes informatiques, techniques et de production pour évaluer correctement les risques cyber et de production, en particulier les incidents liés aux ransomwares. Informer le RSSI pour qu'il puisse définir des priorités, engager un budget et allouer les ressources humaines nécessaires.
3. Élaborer une stratégie pour les fournisseurs technologiques et la plateforme de cybersécurité OT. De nombreuses nouvelles solutions de sécurité émergent sur le marché, mais la pénurie de compétences reste d'actualité. De plus, à mesure que votre posture de sécurité mûrit, rapprochez-vous de fournisseurs disposant d'un large portefeuille de solutions pour fournir des solutions de base d'inventaire et de segmentation des ressources, mais également des solutions plus avancées telles qu'un SOC OT ou la capacité de prendre en charge un SOC IT/OT commun.

Méthodologie de l'étude

La plupart des personnes interrogées ont des titres de postes liés aux opérations de production industrielle, et près d'un tiers d'entre elles sont des vice-présidents ou des directeurs d'usine. La plupart des personnes interrogées, quel que soit leur titre, sont profondément impliquées dans les décisions d'achat en matière de cybersécurité. Et ces profils ont de plus en plus souvent le dernier mot dans les décisions d'achat en matière d'OT. L'enquête de cette année a révélé que 91% des personnes interrogées sont régulièrement impliquées dans les décisions d'achat portant sur la cybersécurité de leur organisation.

Les personnes qui ont participé à l'enquête de cette année évoluent dans l'un des secteurs suivants :

- Production industrielle
- Transports & logistique
- Soins de santé, pharmaceutique
- Pétrole, gaz, raffinage
- Énergie, Utilities
- Chimie, pétrochimie
- Eau, eaux usées

Objectifs de l'étude

Fortinet a fait appel à InMoment, un spécialiste des études de marché, pour dresser le profil type d'un professionnel OT.

L'enquête qui a été menée vise à mieux comprendre les points suivants :

- Le rôle de ce profil au sein des entreprises
- Comment les fonctions de sécurité sont utilisées
- Le suivi et la communication des informations
- Les facteurs d'influence et de réussite

Approche

Le panel interrogé a permis de recueillir 570 questionnaires complets avec le profil suivant de répondants provenant d'une entreprise de :

- Production industrielle
- Transports & logistique
- Soins de santé, pharmaceutique
- Pétrole, gaz, raffinage
- Énergie, Utilities
- Chimie, pétrochimie
- Eau, eaux usées
    - employant plus de 1 000 personnes, à quelques exceptions près
- Les technologies OT relèvent de leurs responsabilités fonctionnelles
- Évolue dans le domaine de production industrielle ou de l'opérationnel en usine

- Est impliqué dans les décisions d'achat en matière de cybersécurité
- Périmètre mondial en 2022 et 2023 :
  - Les personnes interrogées sont originaires de différentes régions du monde : Australie, Nouvelle-Zélande, Brésil, Canada, Égypte, France, Allemagne, Inde, Japon, Mexique, Afrique du Sud, Royaume-Uni et États-Unis.

Conclusion

L'état des lieux 2023 des technologies OT et de leur cybersécurité constate que la cybersécurité OT une priorité pour les entreprises. Cette tendance est importante et nécessaire avec 75 % des entreprises interrogées qui ont dû faire face à au moins une cyberattaque au cours des 12 derniers mois. Les données de l'enquête suggèrent que la cybersécurité OT s'améliore ou arrive à maturité, et que les incidents semblent diminuer. De même, les risques associés aux incidents OT deviennent plus visibles au travers d'événements mondiaux. En outre, les entreprises sont désormais plus agressives dans leur posture de sécurité OT, tandis que les équipes informatiques s'impliquent de plus en plus dans les réseaux industriels.

Les résultats de notre enquête témoignent d'un nombre plus élevé et d'une diversité des solutions de cybersécurité OT. Cette cybersécurité OT, ses modalités de gestion et le déploiement des solutions de sécurité ont gagné en maturité, avec un impact positif à la clé. Mais la plupart des entreprises ont encore un long chemin à parcourir pour se protéger de manière adéquate contre les malwares courants comme les ransomwares.

[1] "What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?," McKinsey and Company, 17 août 2022.

[2] 2022 Global Threat Landscape Report, FortiGuard Labs, 22 février 2023.

[3] "Cyber-Attack Against Ukrainian Critical Infrastructure," CISA, 20 juillet 2021.

[4] "Ukraine: Russian attacks on critical energy infrastructure amount to war crimes," Amnesty International, 22 octobre 2022.

[5] Jonathan Reed, Pipedream Malware Can Disrupt or Destroy Industrial Systems, Security Intelligence, 19 avril 2023.

[6] The 2023 Global Ransomware Report, Fortinet, 24 avril 2023.

[7] 2022 Global Threat Landscape Report, FortiGuard Labs, 22 février 2023.

[8] 2022 State of Operational Technology and Cybersecurity Report, Fortinet, 21 juin 2022.

[9] The 2023 Global Ransomware Report, Fortinet, 24 avril 2023.

[10] CIS Critical Security Controls ICS Companion Guide, Center for Internet Security, Version 7.

juin 22, 2023 8:57 AM
2101968-0-0-FR